HotBrick
Don't Get Hacked. Get HotBrick.
Official Tech Documents
The better way to get your HotBrick product up and running

Firewall HotBrick LB-2 VPN / VPN 600/2

How To

LB-2 IPSec Tunnel with HotBrick VPN 600/2 Setup Guide

USA
7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

EUROPE
Generatorstraat 26
Hengelo (Ov), 7556 RC
Amsterdam - Netherlands
www.hotbrick.nl
support@hotbrick.nl

BRAZIL
Francisco Tramontano, 100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br

LB-2 IPSec Tunnel with HotBrick VPN 600/2 Setup Guide

The HotBrick LB-2 is a VPN capable Dual WAN Gateway with industry standard IPsec encryption. It provides extremely secure LAN-to-LAN connectivity over the Internet. The LB-2 supports VPN by encryption, encapsulation, and authentication using the following methods:

DES/3DES/AES
MD-5
SHA-1/SHA-2

The maximum tunnels allowed are 10 VPN tunnels. This setup guide will help the user establish an IPsec VPN tunnel between an LB-2 VPN and a HotBrick VPN 600/2 or HotBrick 1200/2.

The LB-2 must have the VPN upgrade to establish an IPSec Tunnel.

IPsec Tunnel between an LB-2 VPN and HotBrick VPN 600/2

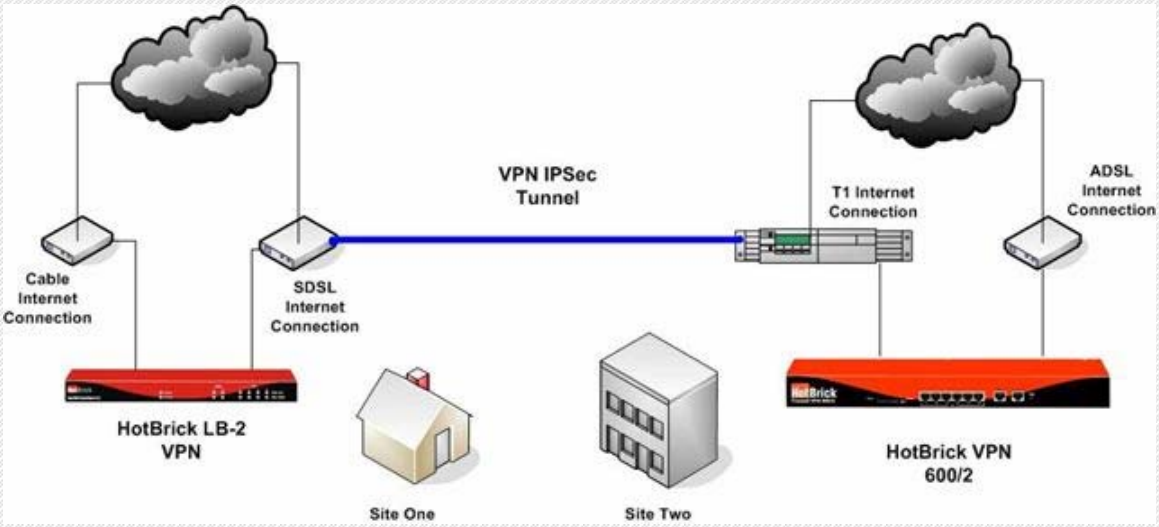

Figure 1 - LB-2 VPN and HotBrick VPN 600/2 IPSec Tunnel

The picture above displays two sites that are joined by a VPN IPsec tunnel between two LB-2 VPN and a VPN 600/2. For the setup below we will be joining the two LAN subnets through the VPN IPSec tunnel. Here is the setup:

1. Login to your firewall
2. Go to Advanced Setup
3. VPN Configuration
4. Global Policy, please see picture below for the global policy for site one:

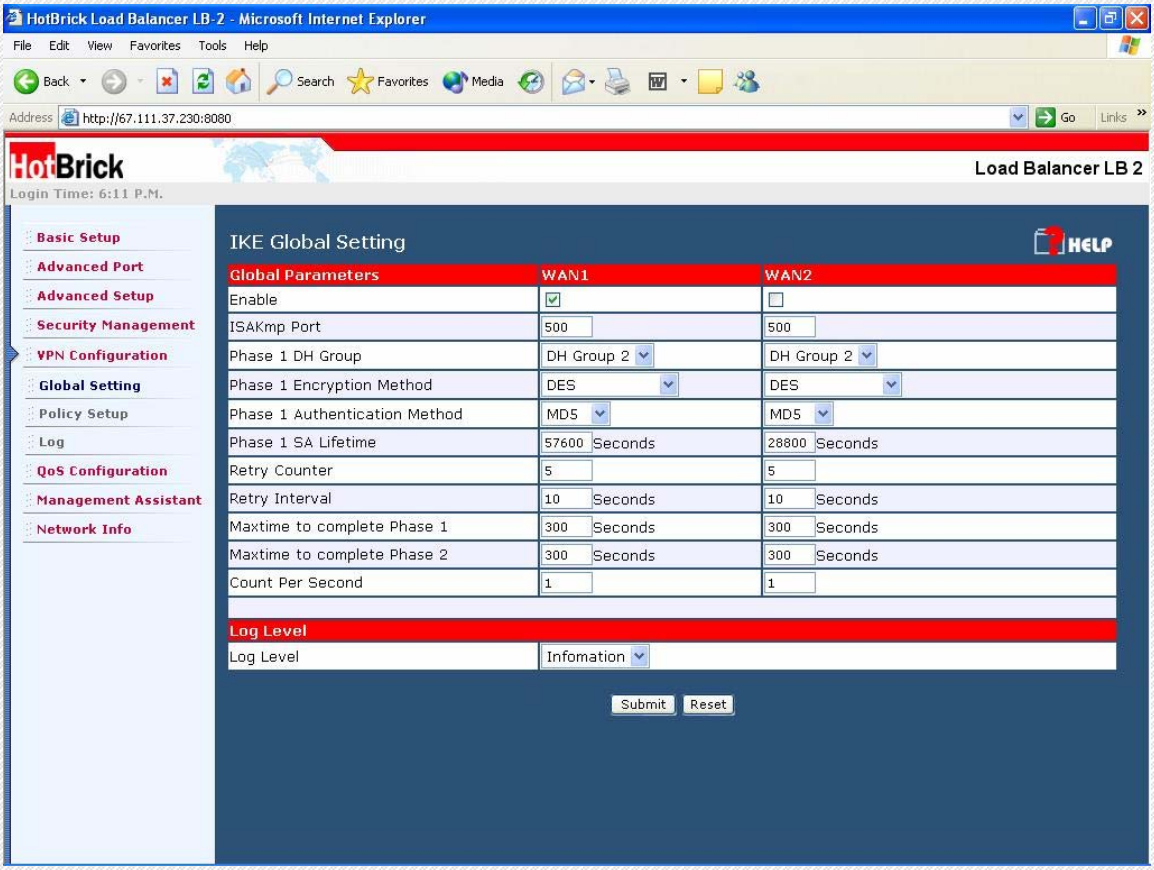

Figure 2 - Global Setting for Site One

5. Under the Global Setting, make sure you enable the interface that you want to Global setting to negotiate at.
6. If you choose to do a redundant tunnel than you can enable both WAN1 and WAN2
7. Since we are connecting to LB-2s via IPsec the default settings are sufficient.
8. Hit Submit
9. The LB-2 will be restarted and refreshed to save the settings.
10. After the settings are refreshed, click on Policy Setup
11. Under IPSec Traffic Binding, input a name for "Tunnel Name". In Figures 3 and 4 below we have the tunnel name "TestLab".
12. Make sure you check the enable box for "Tunnel".
13. For WAN port you can bind the tunnel to WAN1, WAN2 or ANY. If you wish to establish a redundant tunnel then choose ANY.
14. If you have multiple PPPoE sessions on the WAN ports make sure you select the appropriate session.

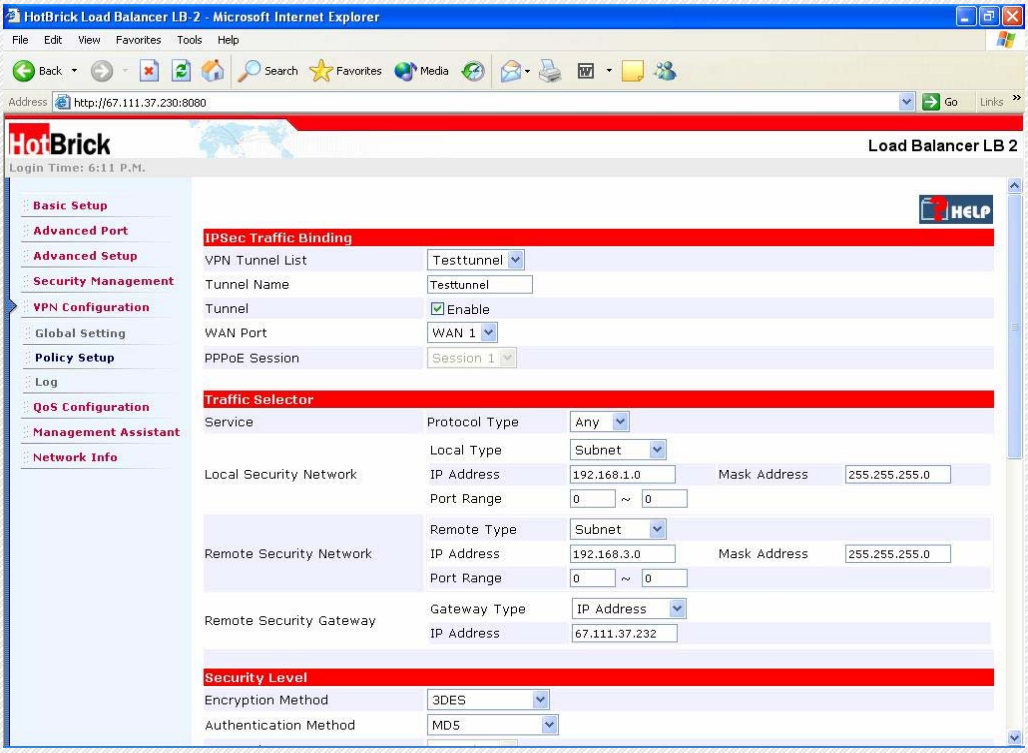

Figure 3 - IPSec Traffic Binding for site one

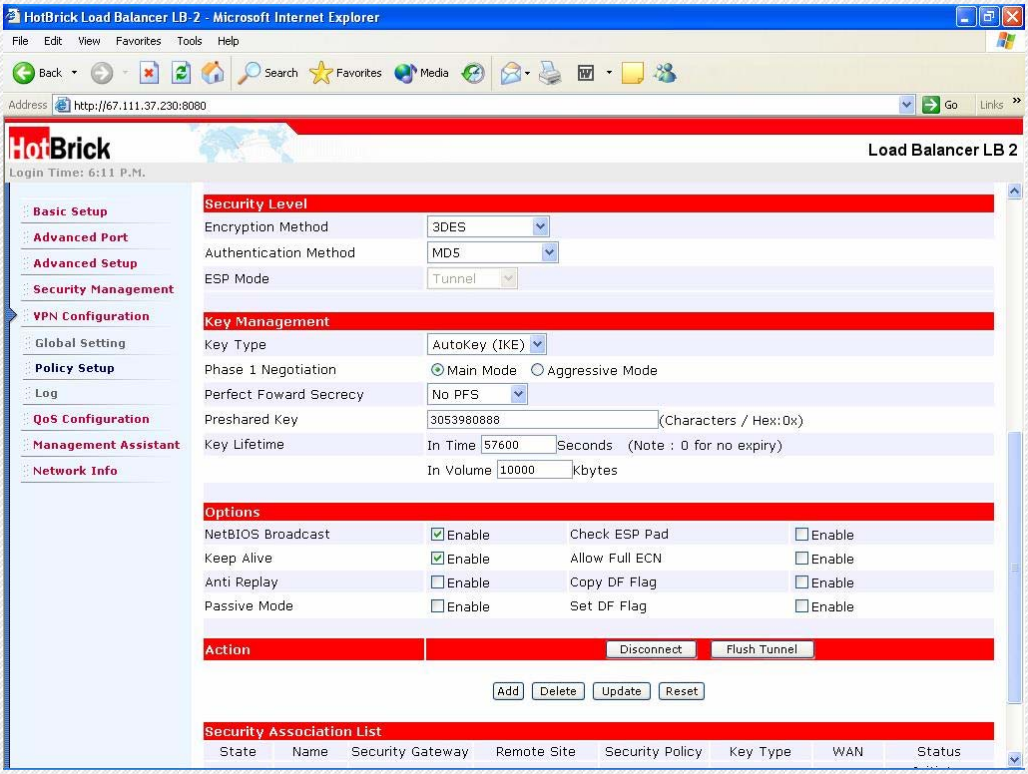
HotBrick Load Balancer LB-2 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://67.111.37.230:8080
Go Links
HotBrick
Load Balancer LB 2
Login Time: 6:11 P.M.
Basic Setup
Advanced Port
Advanced Setup
Security Management
VPN Configuration
Global Setting
Policy Setup
Log
QoS Configuration
Management Assistant
Network Info
Security Level
Encryption Method 3DES
Authentication Method MD5
ESP Mode Tunnel
Key Management
Key Type AutoKey (IKE)
Phase 1 Negotiation Main Mode Aggressive Mode
Perfect Foward Secrecy No PFS
Preshared Key 3053980888 (Characters / Hex:0x)
Key Lifetime In Time 57600 Seconds (Note : 0 for no expiry)
In Volume 10000 Kbytes
Options
NetBIOS Broadcast Enable Check ESP Pad Enable
Keep Alive Enable Allow Full ECN Enable
Anti Replay Enable Copy DF Flag Enable
Passive Mode Enable Set DF Flag Enable
Action Disconnect Flush Tunnel
Add Delete Update Reset
Security Association List
State Name Security Gateway Remote Site Security Policy Key Type WAN Status

Figure 4 - IPSec Traffic Binding for site two

15. Under Traffic Selector, for Service – Protocol Type select "ANY".
16. Under Local Security Network , for Local Type select subnet
17. The IP address must reflect the entire subnet. In Figure 3 and Figure 4:

a. Site One IP address is 192.168.1.0 and Mask Address 255.255.255.0
b. Site Two IP address is 192.168.2.0 and Mask Address 255.255.255.0
c. NOTE – LAN subnets and IP addresses must be different or there will be overlapping.

18. The Port Range can be left at 0 ~ 0.
19. For Remote Security Network, for Remote Type select Subnet.
20. The IP address must again reflect the entire subnet. In our example the remote security network for Site One is 192.168.1.0, and for Site two its 192.168.2.0. Please see Figure 3 and Figure 4.
21. For the Remote Security Gateway the gateway type is IP Address unless you have a Domain Name registered for the remote gateway of the other site's LB-2.
22. Under Security Level, the VPN IPSec Tunnel will always be in ESP (Encapsulating Security Payload) mode.
23. For the Encryption method you can choose from: Null, DES/3DES, or AES. In our example we have chosen 3DES. Please see figure 5 and figure 6.
24. For the Authentication Method you can choose from: Null, MD5, SHA-1/SHA-2. In our example we have chosen SHA-1.

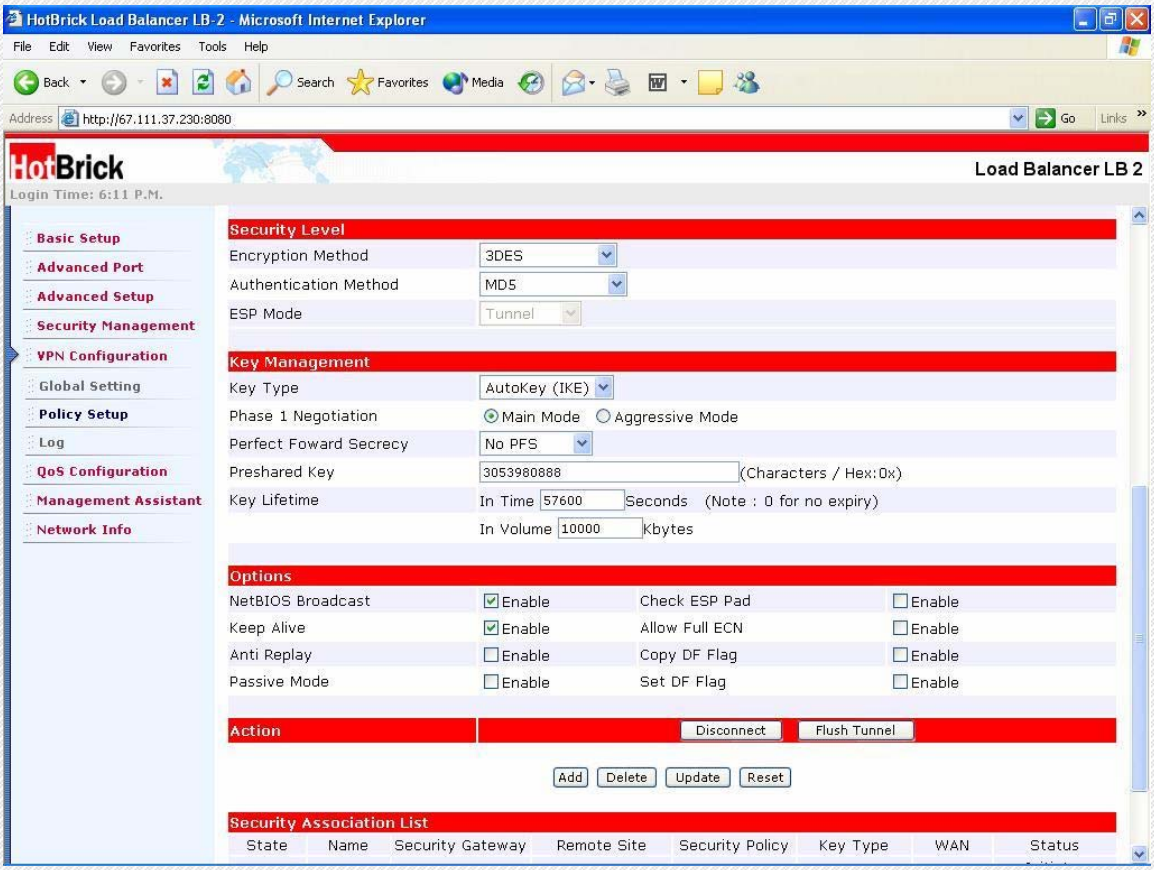

Figure 5 - Policy Setup for site one

25. Under Key Management there are two types: Autokey (IKE) or Manual Key.
26. If AutoKey (IKE), your Phase 1 Negotiation can be Main Mode or Aggressive Mode. In our example we used Main Mode.

27. For Perfect Forward Secrecy you can choose to enable it or not. In our example we have not.
28. The Preshared Key must be characters and/or hexadecimal units. The preshared key entered in our example is 3053980888.
29. The Key life time can be set in seconds with zero indicating no expirations. In our example we used 57600 seconds or eight hours.
30. In Volume is default 10000 Kbytes, it is also optional to input 0 (zero) Kbytes.
31. Since we wanted to browse our network we have enabled Netbios Traffic under "Options", and we enabled keep alive for our Alive Indicator.
32. Once all these values all entered you click on Add.

HotBrick VPN 600/2 Setup

1. Please go to Advanced Setup, then VPN
2. Under the Status page make sure that Tunnel Status is at "Enable"
3. Hit Update

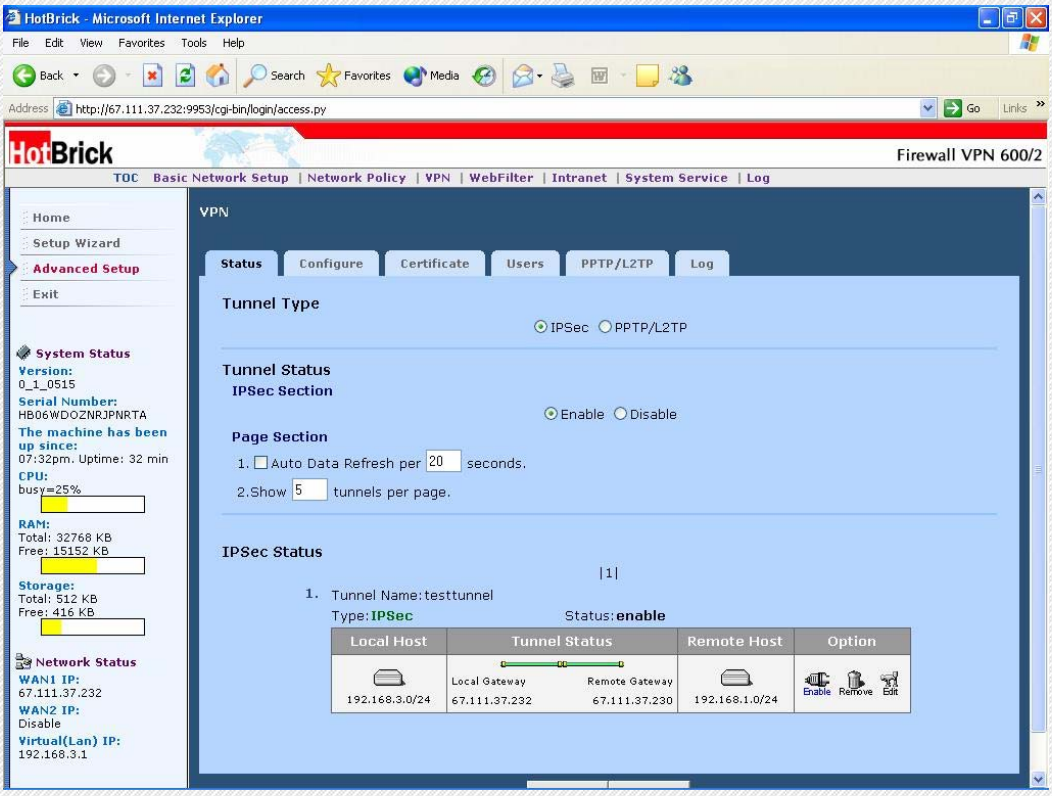

Figure 6 – VPN Status page of HotBrick 600/2

4. Click on the Configure Tab
5. Input a name for the Tunnel. Our example is "testtunnel"
6. Input the "Pre-Shared Key". Our example is "3053980888"

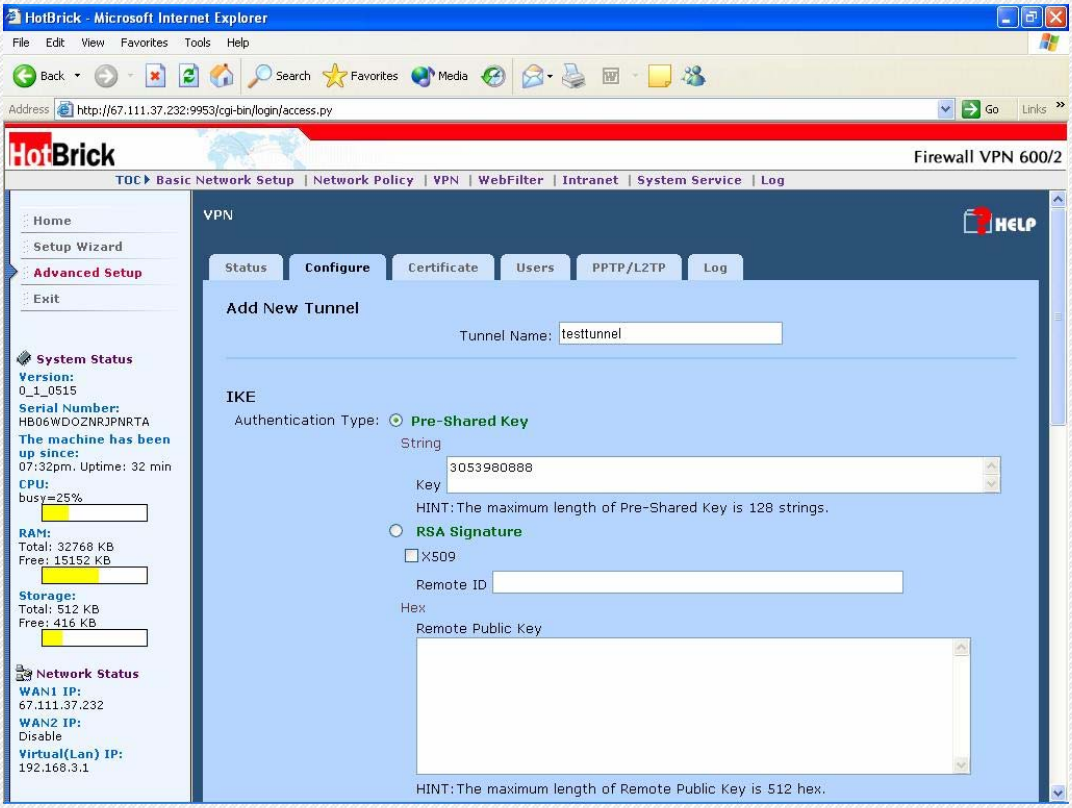

Figure 7 – VPN Configure page of HotBrick 600/2

7. Make sure the key life is "57600" second for the Key life.
8. For the IPSec Section make sure that you select:
a. ESP Encryption
b. ESP Authentication
9. Make sure that the key life for the IPSec section is "57600"seconds for the key life.

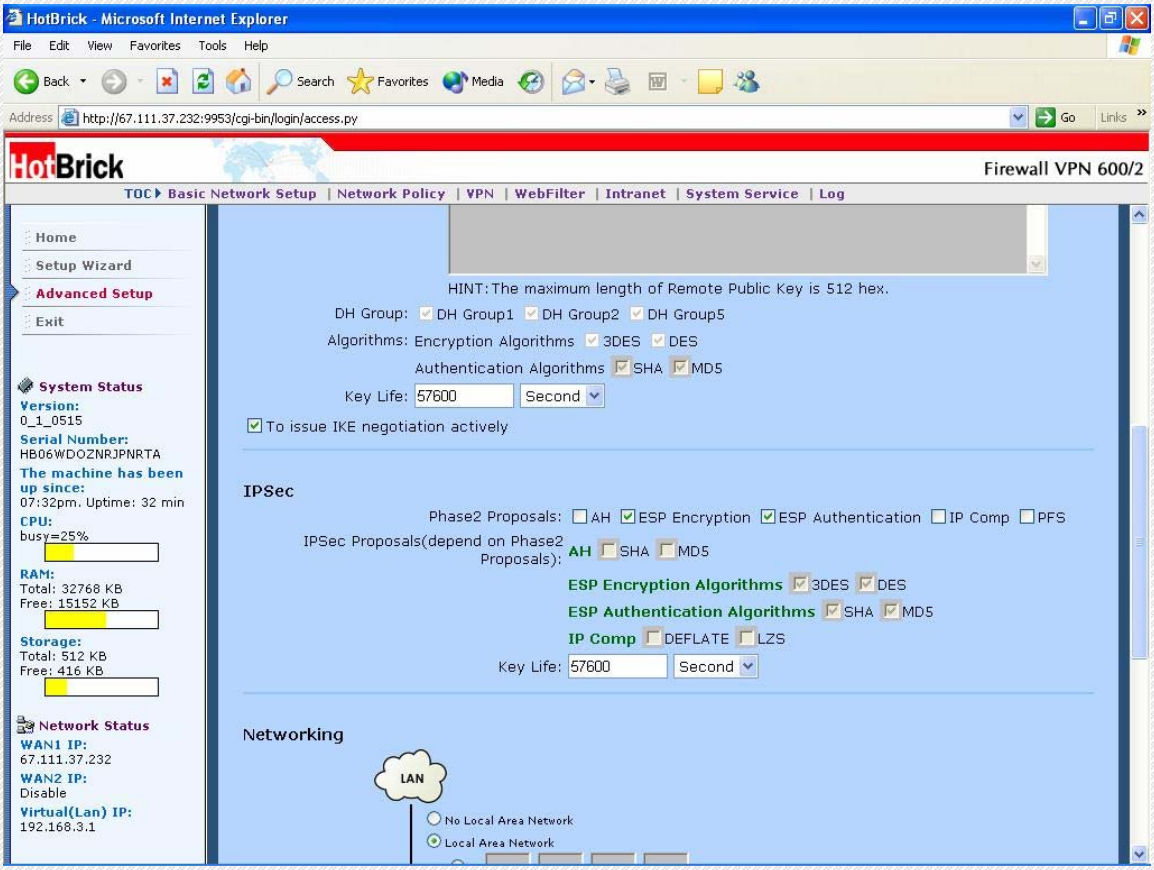

Figure 8 – VPN Configure page of HotBrick 600/2 continued..

10. Under Networking for the Local Area Network make sure subnet is selected.
11. Input the subnet of the HotBrick VPN 600/2. In our example it is 192.168.3.0 and subnet mask 255.255.255.0.
12. Under Remote VPN Gateway IP is the IP address of the LB-2 VPN.
13. Make sure Remote Area Network is selected, and the subnet is also selected.
14. Input the subnet of the LB-2 VPN. In our example is 192.168.1.0 with subnet mask 255.255.255.0.
15. Hit Update

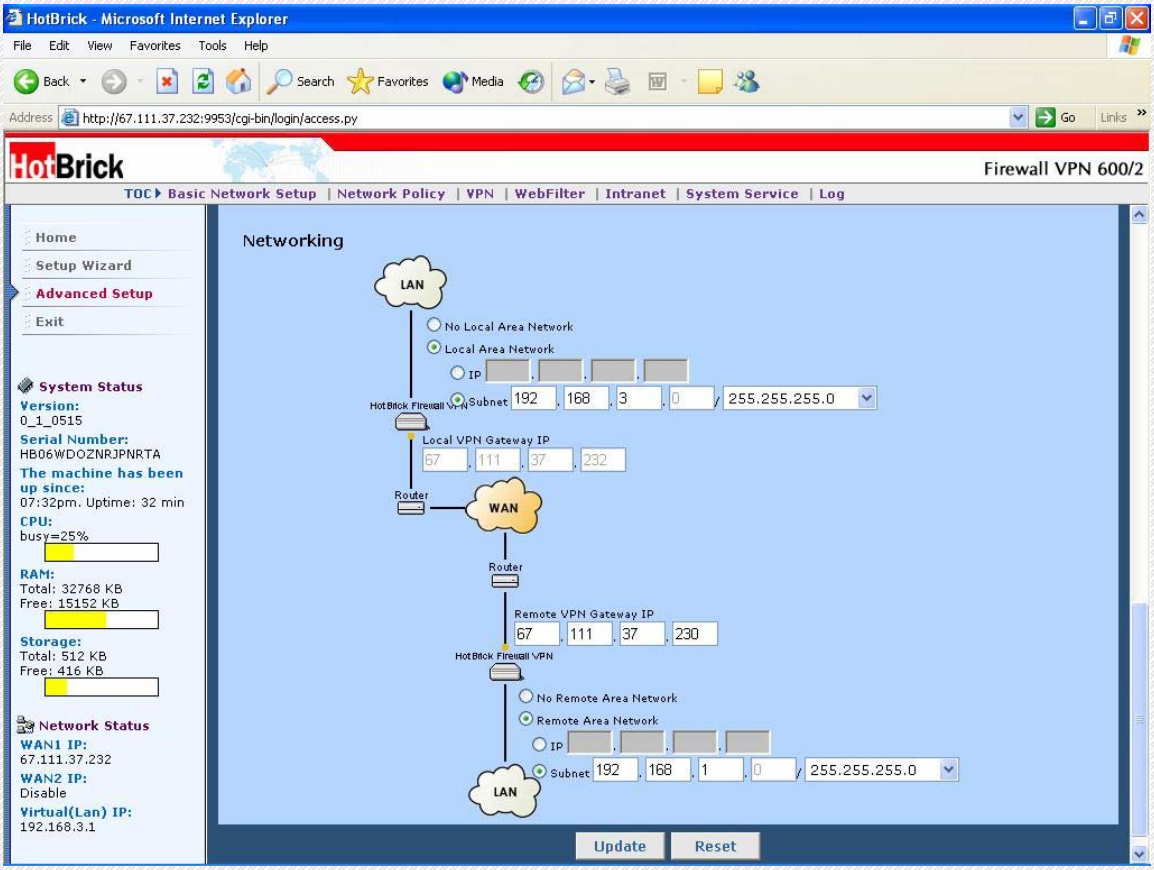

Figure 9 – VPN Configure page of HotBrick 600/2 continued..

16. When you have finished, click connect on the LB-2 VPN. The Figures 10 shows the log with all the phases of the IPSec tunnel established. Figure 11 shows the VPN established on the Home Page of the HotBrick VPN 600/2.

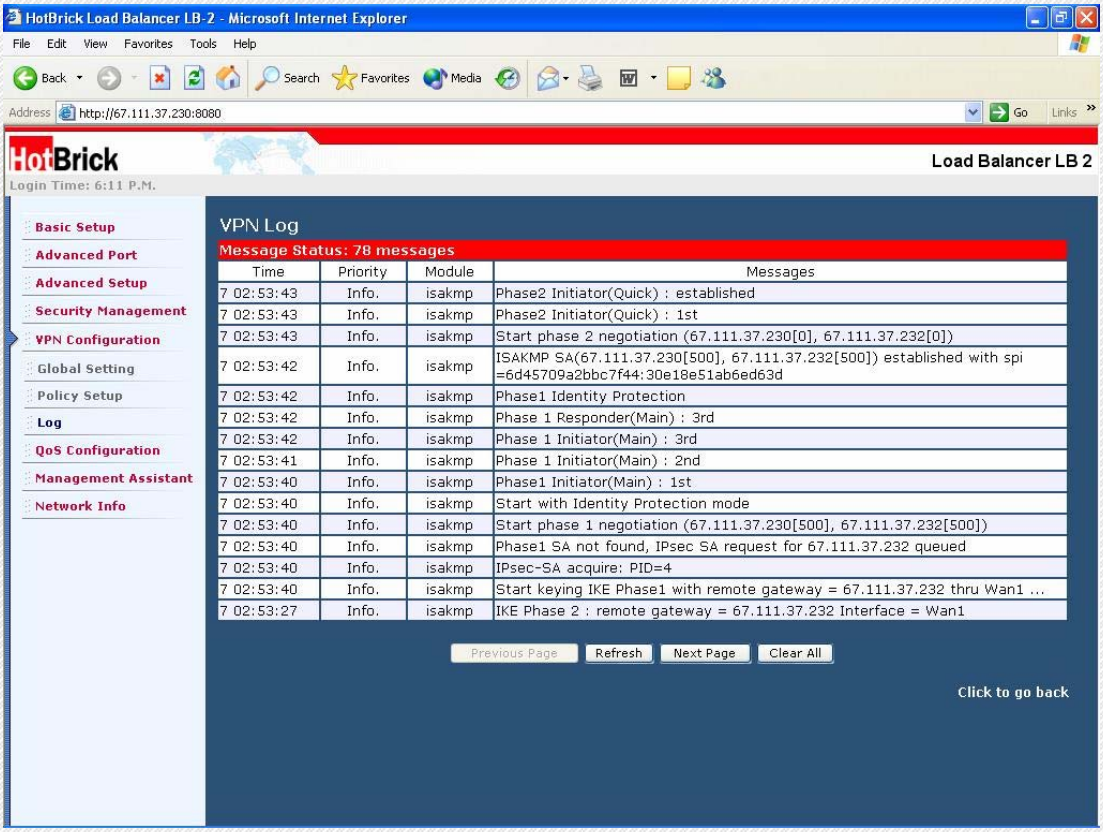
HotBrick Load Balancer LB-2 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://67.111.37.230:8080
Go Links
HotBrick
Load Balancer LB 2
Login Time: 6:11 P.M.
Basic Setup
Advanced Port
Advanced Setup
Security Management
VPN Configuration
Global Setting
Policy Setup
Log
QoS Configuration
Management Assistant
Network Info
VPN Log
Message Status: 78 messages
Time | Priority | Module | Messages
7 02:53:43 | Info. | isakmp | Phase2 Initiator(Quick) : established
7 02:53:43 | Info. | isakmp | Phase2 Initiator(Quick) : 1st
7 02:53:43 | Info. | isakmp | Start phase 2 negotiation (67.111.37.230[0], 67.111.37.232[0])
7 02:53:42 | Info. | isakmp | ISAKMP SA(67.111.37.230[500], 67.111.37.232[500]) established with spi =6d45709a2bbc7f44:30e18e51ab6ed63d
7 02:53:42 | Info. | isakmp | Phase1 Identity Protection
7 02:53:42 | Info. | isakmp | Phase 1 Responder(Main) : 3rd
7 02:53:42 | Info. | isakmp | Phase 1 Initiator(Main) : 3rd
7 02:53:41 | Info. | isakmp | Phase 1 Initiator(Main) : 2nd
7 02:53:40 | Info. | isakmp | Phase1 Initiator(Main) : 1st
7 02:53:40 | Info. | isakmp | Start with Identity Protection mode
7 02:53:40 | Info. | isakmp | Start phase 1 negotiation (67.111.37.230[500], 67.111.37.232[500])
7 02:53:40 | Info. | isakmp | Phase1 SA not found, IPsec SA request for 67.111.37.232 queued
7 02:53:40 | Info. | isakmp | IPsec-SA acquire: PID=4
7 02:53:40 | Info. | isakmp | Start keying IKE Phase1 with remote gateway = 67.111.37.232 thru Wan1 ...
7 02:53:27 | Info. | isakmp | IKE Phase 2 : remote gateway = 67.111.37.232 Interface = Wan1
Previous Page
Refresh
Next Page
Clear All
Click to go back

Figure 10 – LB-2 VPN log with VPN tunnel established

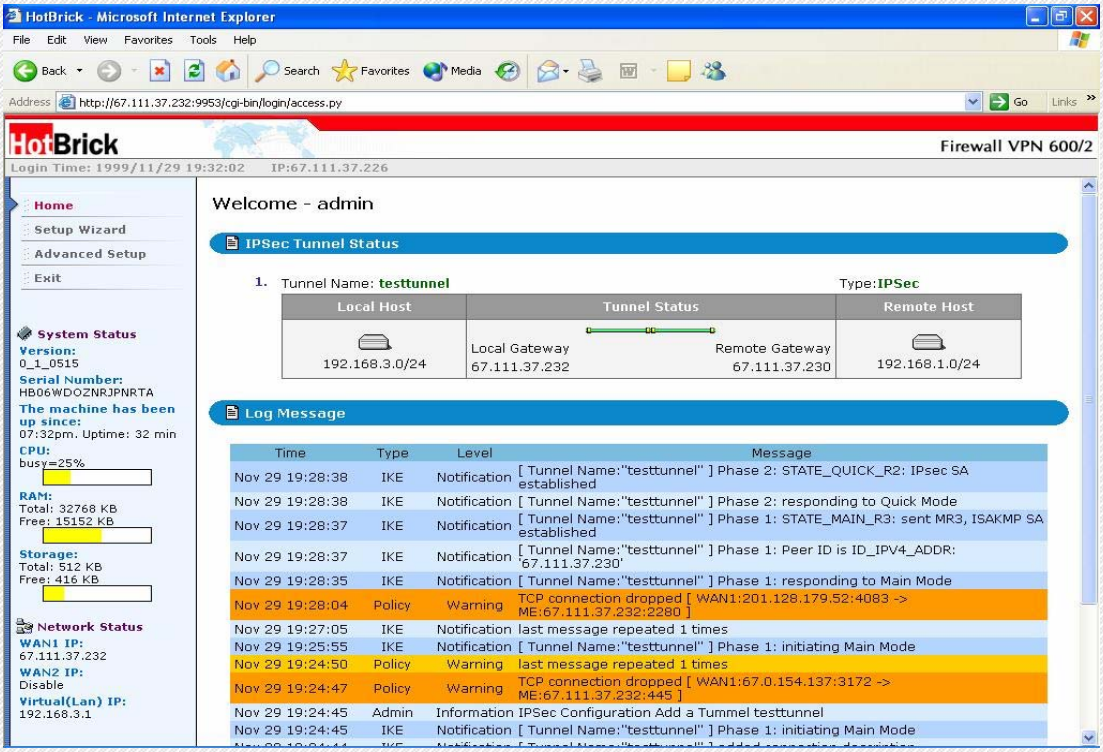
HotBrick - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://67.111.37.232:9953/cgi-bin/login/access.py
Go Links
HotBrick
Firewall VPN 600/2
Login Time: 1999/11/29 19:32:02 IP:67.111.37.226
Home
Setup Wizard
Advanced Setup
Exit
System Status
Version:
0_1_0515
Serial Number:
HB06WDOZNRJPNRTA
The machine has been up since:
07:32pm. Uptime: 32 min
CPU:
busy=25%
RAM:
Total: 32768 KB
Free: 15152 KB
Storage:
Total: 512 KB
Free: 416 KB
Network Status
WAN1 IP:
67.111.37.232
WAN2 IP:
Disable
Virtual(Lan) IP:
192.168.3.1
Welcome - admin
IPSec Tunnel Status
1. Tunnel Name: testtunnel
Type:IPSec
Local Host | Tunnel Status | Remote Host
192.168.3.0/24
Local Gateway 67.111.37.232
Remote Gateway 67.111.37.230
192.168.1.0/24
Log Message
Time | Type | Level | Message
Nov 29 19:28:38 | IKE | Notification | [Tunnel Name:"testtunnel"] Phase 2: STATE_QUICK_R2: IPsec SA established
Nov 29 19:28:38 | IKE | Notification | [Tunnel Name:"testtunnel"] Phase 2: responding to Quick Mode
Nov 29 19:28:37 | IKE | Notification | [Tunnel Name:"testtunnel"] Phase 1: STATE_MAIN_R3: sent MR3, ISAKMP SA established
Nov 29 19:28:37 | IKE | Notification | [Tunnel Name:"testtunnel"] Phase 1: Peer ID is ID_IPV4_ADDR: '67.111.37.230'
Nov 29 19:28:35 | IKE | Notification | [Tunnel Name:"testtunnel"] Phase 1: responding to Main Mode
Nov 29 19:28:04 | Policy | Warning | TCP connection dropped [WAN1:201.128.179.52:4083 -> ME:67.111.37.232:2280]
Nov 29 19:27:05 | IKE | Notification | last message repeated 1 times
Nov 29 19:25:55 | IKE | Notification | [Tunnel Name:"testtunnel"] Phase 1: initiating Main Mode
Nov 29 19:24:50 | Policy | Warning | last message repeated 1 times
Nov 29 19:24:47 | Policy | Warning | TCP connection dropped [WAN1:67.0.154.137:3172 -> ME:67.111.37.232:445]
Nov 29 19:24:45 | Admin | Information | IPSec Configuration Add a Tummel testtunnel
Nov 29 19:24:45 | IKE | Notification | [Tunnel Name:"testtunnel"] Phase 1: initiating Main Mode

Figure 11 – Home Page of VPN 600/2 with VPN tunnel established.